Welcome to the PIA for FY 2011!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vaww.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the VA Directive 6508 referenced in the procedure section of this document.

a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Directive 6508.

b. Records Officer is responsible for supplying records retention and deletion schedules.

c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Directive 6508 and to immediately report all anomalies to the Privacy Service and appropriate management chain.

d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.

e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect indentify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

Microsoft Office 2003: To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

Microsoft Office 2007: To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable

All Macros; 2) Click OK

Final Signatures

Final Signatures are digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.

Privacy Impact Assessment Uploaded into SMART

Privacy Impact Assessments should be uploaded into C&A section of SMART.
All PIA Validation Letters should be emailed to christina.pettit@va.gov to received full credit for submission.

(FY 2011) PIA: System Identification

Program or System Name:	CDCO > AITC > VHA > National Canteen Service > VCS AIS
OMB Unique System / Application / Program Identifier	029-00-02-00-01-1120-00
Description of System/ Application/ Program:	This system handles the entire VCS operation. Cash Register system, financial, procurement, human resources, payroll deduction and all other VCS operations. Personal Identifiable Information is in the following modules, payroll deduction; treasury offset program and human resource modules. (See additional comments tab for sub-applications that make up VCS AIS)
Facility Name:	Austin Information Technology Center (AITC)

Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	512-326-6217	amy.howe1@va.gov
Information Security Officer:	Thomas P. Johnson	314-845-1446	Thomas.P.Johnson@va.gov
System Owner/ Chief Information Officer:	John Rucker	512-326-6422	john.rucker@va.gov
Information Owner:	Craig Caruso	314-845--1340	craig.caruso@va.gov
Other Titles: AITC Program Manager	Cindy Mack	512-326-6854	cindy.mack@va.gov
Person Completing Document:	Analida Aguilar	512-326-6023	analida.aguilar@va.gov
Other Titles:			

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	02/2009
Date Approval To Operate Expires:	11/2010
What specific legal authorities authorize this program or system:	1) Title 38, United States Code, Part V, Chapter 78 2) 3936-2 Public Law 108-422
What is the expected number of individuals that will have their PII stored in this system:	240,000
Identify what stage the System / Application / Program is at:	Operations/Maintenance
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.	3 years
Is there an authorized change control process which documents any changes to existing applications or systems?	Yes
If No, please explain:	
Has a PIA been completed within the last three years?	Yes
Date of Report (MM/YYYY):	11/2010

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.

- ☑ Have any changes been made to the system since the last PIA?
- ☑ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- ☑ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- ☑ Does this system/application/program collect, store or disseminate PII/PHI data?
- ☑ Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system , please complete TAB 7 & TAB 12. (See Comment for Definition of PII)

(FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.

For each applicable System(s) of Records, list:

1. All System of Record Identifier(s) (number):

2. Name of the System of Records:
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?

Does the System of Records Notice require modification or updating?

Is PII collected by paper methods?
Is PII collected by verbal methods?
Is PII collected by automated methods?
Is a Privacy notice provided?
Proximity and Timing: Is the privacy notice provided at the time of data collection?
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

Yes
117VA103 Veteran Canteen Service (VCS) Payroll Deduction System - VA http://www.rms.oit.va.gov/SOR_Records/117VA103.pdf
Yes
No
(Please Select Yes/No)
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No

(FY 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Electronic/File Transfer	The information collected on this form will be used by VCS to identify you as an authorized VA employee customer eligible to participate in the Payroll Deduction Program (PDP); to establish a PDP account on your behalf; and to the administer PDP account transactions. Executive Order 9397 authorizes collection of your Social Security Number. Information collected may be disclosed to authorized VCS/VA employees responsible for administering and recording purchase and payment transactions to your PDP account.	Automated	Automated
Family Relation (spouse, children, parents, grandparents, etc)	N/A			
Service Information	N/A			
Medical Information	N/A			
Criminal Record Information	N/A			
Guardian Information	N/A			
Education Information	VA File Database	The information collected on this form will be used by VCS to identify you as an authorized VA employee customer eligible to participate in the Payroll Deduction Program (PDP); to establish a PDP account on your behalf; and to the administer PDP account transactions. Executive Order 9397 authorizes collection of your Social Security Number. Information collected may be disclosed to authorized VCS/VA employees responsible for administering and recording purchase and payment transactions to your PDP account.	Automated	Automated
Benefit Information	N/A			
Other (Explain)				

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Voluntary	Last name, first name, SSN, telephone number, email address. To authenticate subject to system and inform subject about specials and other new services.
Family Relation (spouse, children, parents, grandparents, etc)	No			
Service Information	No			
Medical Information	No			
Criminal Record Information	No			
Guardian Information	No			
Education Information	Yes	VA Files / Databases (Identify file)	Voluntary	Last name, first name, SSN, telephone number, email address. To authenticate subject to system and inform subject about specials and other new services.
Benefit Information	No			
Credit Card Information	Yes	VA Files / Databases (Identify file)	Mandatory	On the form
Electronic Payroll Deduction	Yes	VA Files / Databases (Identify file)	Mandatory	On the form
Other (Explain)				

(FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VA National Enrollment Database (NED)	No	This information is used to authenticate the veteran against the Database (PAID and NED). This is information is not stored on VA Systems. If customer is not a VA employee, the stored procedure will query the NED Database with the SSN to determine if the customer is an enrolled veteran. If the SSN is found, a customer number will be generated and returned to the web service along with the veteran's first name, middle initial and last name. Eligibles are then notified about specials and other new services.	PII	ISA/MOU

Internal Sharing: VA Organization	VA PAID	No	This information is used to authenticate the veteran against the Database (PAID and NED). This is information is not stored on VA Systems. If customer is not a VA employee, the stored procedure will query the NED Database with the SSN to determine if the customer is an enrolled veteran. If the SSN is found, a customer number will be generated and returned to the web service along with the veteran's first name, middle initial and last name. Eligibles are then notified about specials and other new services.	PII	Security Policy for PAID, Version 1, February 2009 and Handbook 6500
Other Federal Government Agency		No			
State Government Agency		No			
Local Government Agency		No			
Research Entity		No			
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2011) PIA: Access to Records

Does the system gather information from another system?	Yes
Please enter the name of the system:	PAID/NED
Per responses in Tab 4, does the system gather information from an individual?	
If information is gathered from an individual, is the information provided:	☐ Through a Written Request ☑ Submitted in Person ☑ Online via Electronic Form
Is there a contingency plan in place to process information when the system is down?	Yes

(FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?	Yes
if yes, please check all that apply:	☐ Drug/Alcohol Counseling ☐ Mental Health ☐ HIV ☐ Research ☐ Sickle Cell ☑ Other (Please Explain)

Describe process for authorizing access to this data.

Answer: At this time individuals can not access their information. System users and administrators cannot access their own data. Application access controls and NTFS file access controls.

(FY 2011) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public? No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: Fields on web forms are identified and limited to what information can be entered

How is data checked for completeness?

Answer: It is verified against existing databases.

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer: Files are updated once to twice a month.

How is new data verified for relevance, authenticity and accuracy?

Answer: It is checked against current database.

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: Some records are kept forever and some records are deleted when employee resigns or retires.

Explain why the information is needed for the indicated retention period?

Answer: The records are retained to have proof to customer that they agreed to the terms, if they would have a dispute.

What are the procedures for eliminating data at the end of the retention period?

Answer: System programming handles this automatically based on updates received from VA systems.

Where are these procedures documented?

Answer: Deputy Under Secretary for Health for Operations And Management (DUSHOM) on Media Sanitization, September 6, 2006.
Media Sanitization and Destruction Users Guide v2.1
AITC Handbook 6500.5, NIST SP 800-88 provides guidance on media sanitization.

How are data retention procedures enforced?

Answer: VA Handbook 6500, Information Security Program, Appendix D.3.g.(7)(c), MP-6 Sanitization Compliance."

Has the retention schedule been approved by the National Archives and Records Administration (NARA) Yes

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2011) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13? No

If Yes, How will parental or guardian approval be obtained?

Answer:

(FY 2011) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.	Yes
Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..	Yes
Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes

If 'No' to any of the 3 questions above, please describe why:
Answer:

Is adequate physical security in place to protect against unauthorized access?	Yes

If 'No' please describe why:
Answer:

Explain how the project meets IT security requirements and procedures required by federal law.
Answer: VCS AIS is housed at Austin ITC and complies with designated IT security requirements and procedures as directed by federal law. From VA Directive 6500, Information Security Program: The security of VA information and information systems is vital to the success of VA's mission. To that end, VA shall establish and maintain a comprehensive Department-wide information security program to provide for development and maintenance of cost-effective security controls needed to protect VA information, in any media or format, and VA information systems. The VA information security program shall include the following elements: Periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the Department. Policies and procedures that (a) are based on risk assessments (b) cost-effectively reduce security risks to an acceptable level and, (c) ensure that information security is addressed throughout the life cycle of each system information security is addressed throughout the life cycle of each system.

Explain what security risks were identified in the security assessment? *(Check all that apply)*

- [x] Air Conditioning Failure
- [ ] Chemical/Biological Contamination
- [ ] Blackmail
- [ ] Bomb Threats
- [ ] Burglary/Break In/Robbery
- [x] Cold/Frost/Snow
- [x] Communications Loss
- [x] Computer Intrusion
- [x] Computer Misuse
- [x] Data Destruction
- [x] Data Disclosure
- [x] Data Integrity Loss
- [x] Denial of Service Attacks
- [ ] Earthquakes
- [x] Eavesdropping/Interception
- [x] Errors (Configuration and Data Entry)
- [x] Fire (False Alarm, Major, and Minor)
- [x] Flooding/Water Damage
- [ ] Fraud/Embezzlement
- [x] Hardware Failure
- [ ] Identity Theft
- [x] Malicious Code
- [x] Power Loss
- [ ] Sabotage/Terrorism
- [x] Storms/Hurricanes
- [ ] Substance Abuse
- [x] Theft of Assets
- [x] Theft of Data
- [ ] Vandalism/Rioting

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

- ☑ Access Control
- ☑ Audit and Accountability
- ☑ Awareness and Training
- ☑ Certification and Accreditation Security Assessments
- ☑ Configuration Management
- ☑ Contingency Planning
- ☑ Identification and Authentication
- ☑ Incident Response
- ☑ Media Protection
- ☑ Personnel Security
- ☑ Physical and Environmental Protection
- ☐ Risk Management

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.
Answer:

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☐	The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☑	The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☐	The potential impact is **high** if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☑	The potential impact is **moderate** if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is **low** if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.
Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? **(Choose One)**	☑	The potential impact is **high** if the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☐	The potential impact is **moderate** if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is **low** if the loss of confidentiality could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments?

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Please add additional controls:

(FY 2011) PIA: Additional Comments

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.

Tab 2, line 5 - The VCS AIS is comprised of: Automated Sales Reporting (ASR), Electronic Card System (ECD), Electronic Payroll Deduction (EPD), Financial Management Information System (FMI), Inventory Management System (IMS), Purchase Order Management System (POM), Veterans Canteen Web (VCW). All of which share an architectural environment within the AITC General Support System.

Tab 4, line 7 - Collection methods: Paper forms, Web forms, File Database, Electronic File Transfer, Telephone.

Tab 5, line 35 - To advise subjects of specials and provide information.

(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system?

Access Manager	X	Automated Sales Reporting (ASR)		Automated Folder Processing System (AFPS)
Actuarial		BCMA Contingency Machines		Automated Medical Information Exchange II (AIME II)
Appraisal System		Benefits Delivery Network (BDN)		Automated Medical Information System (AMIS)290
ASSISTS		Centralized Property Tracking System		Automated Standardized Performace Elements Nationwide (ASPEN)
Awards		Common Security User Manager (CSUM)		Centralized Accounts Receivable System (CARS)
Awards		Compensation and Pension (C&P)		Committee on Waivers and Compromises (COWC)
Baker System		Control of Veterans Records (COVERS)		Compensation and Pension (C&P) Record Interchange (CAPRI)
Bbraun (CP Hemo)		Control of Veterans Records (COVERS)		Compensation & Pension Training Website
BDN Payment History		Control of Veterans Records (COVERS)		Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
BIRLS		Courseware Delivery System (CDS)		Distribution of Operational Resources (DOOR)
C&P Payment System		Dental Records Manager		Educational Assistance for Members of the Selected Reserve Program CH 1606
C&P Training Website		Education Training Website		Electronic Performance Support System (EPSS)
CONDO PUD Builder		Electronic Appraisal System		Enterprise Wireless Messaging System (Blackberry)
Corporate Database	X	Electronic Card System (ECS)	X	Financial Management Information System (FMI)
Data Warehouse	X	Electronic Payroll Deduction (EPD)		Hearing Officer Letters and Reports System (HOLAR)
EndoSoft		Eligibility Verification Report (EVR)		Inquiry Routing Information System (IRIS)
FOCAS		Fiduciary Beneficiary System (FBS)		Modern Awards Process Development (MAP-D)
Inforce		Fiduciary STAR Case Review		Personnel and Accounting Integrated Data and Fee Basis (PAID)
INS - BIRLS		Financial and Accounting System (FAS)		Personal Computer Generated Letters (PCGL)
Insurance Online		Insurance Unclaimed Liabilities		Personnel Information Exchange System (PIES)
Insurance Self Service	X	Inventory Management System (IMS)		Personnel Information Exchange System (PIES)
LGY Home Loans		LGY Centralized Fax System		Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing		Loan Service and Claims	X	Purchase Order Management System (POMS)
Mobilization		Loan Guaranty Training Website		Reinstatement Entitelment Program for Survivors (REAPS)
Montgomery GI Bill		Master Veterans Record (MVR)		Reserve Educational Assistance Program CH 1607
MUSE		Mental Health Asisstant		Service Member Records Tracking System
Omnicell		National Silent Monitoring (NSM)		Survivors and Dependents Education Assistance CH 35
Priv Plus		Powerscribe Dictation System		Systematic Technical Accuracy Review (STAR)
RAI/MDS		Rating Board Automation 2000 (RBA2000)		Training and Performance Support System (TPSS)
Right Now Web		Rating Board Automation 2000 (RBA2000)		VA Online Certification of Enrollment (VA-ONCE
SAHSHA		Rating Board Automation 2000 (RBA2000)		VA Reserve Educational Assistance Program
Script Pro		Records Locator System		Veterans Appeals Control and Locator System (VACOLS)
SHARE		Review of Quality (ROQ)		Veterans Assistance Discharge System (VADS)
SHARE		Search Participant Profile (SPP)		Veterans Exam Request Info System (VERIS)
SHARE		Spinal Bifida Program Ch 18		Veterans Service Representative (VSR) Advisor
Sidexis		State Benefits Reference System		Vocational Rehabilitation & Employment (VR&E) CH 31

	Synquest	State of Case/Supplemental (SOC/SSOC)	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
	VBA Data Warehouse	Telecare Record Manager	Web Automated Folder Processing System (WAFPS)
	VBA Training Academy	VBA Enterprise Messaging System	Web Automated Reference Material System (WARMS)
X	Veterans Canteen Web	Veterans On-Line Applications (VONAPP)	Web Automated Verification of Enrollment
	VIC	Veterans Service Network (VETSNET)	Web-Enabled Approval Management System (WEAMS)
	VR&E Training Website	Web Electronic Lender Identification	Web Service Medical Records (WebSMR)
	Web LGY		Work Study Management System (WSMS)

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?

ASISTS	Beneficiary Travel	Accounts Receivable	Adverse Reaction Tracking
Bed Control	Care Management	ADP Planning (PlanMan)	Authorization/ Subscription
CAPRI	Care Tracker	Bad Code Med Admin	Auto Replenishment/ Ward Stock
CMOP	Clinical Reminders	Clinical Case Registries	Automated Info Collection Sys
Dental	CPT/ HCPCS Codes	Clinical Procedures	Automated Lab Instruments
Dietetics	DRG Grouper	Consult/ Request Tracking	Automated Med Info Exchange
Fee Basis	DSS Extracts	Controlled Substances	Capacity Management - RUM
GRECC	Education Tracking	Credentials Tracking	Capacity Management Tools
HINQ	Engineering	Discharge Summary	Clinical Info Resource Network
IFCAP	Event Capture	Drug Accountability	Clinical Monitoring System
Imaging	Extensible Editor	EEO Complaint Tracking	Enrollment Application System
Kernal	Health Summary	Electronic Signature	Equipment/ Turn-in Request
Kids	Incident Reporting	Event Driven Reporting	Gen. Med.Rec. - Generator
Lab Service	Intake/ Output	External Peer Review	Health Data and Informatics
Letterman	Integrated Billing	Functional Independence	ICR - Immunology Case Registry
Library	Lexicon Utility	Gen. Med. Rec. - I/O	Income Verification Match
Mailman	List Manager	Gen. Med. Rec. - Vitals	Incomplete Records Tracking
Medicine	Mental Health	Generic Code Sheet	Interim Mangement Support
MICOM	MyHealthEVet	Health Level Seven	Master Patient Index VistA
NDBI	National Drug File	Hospital Based Home Care	Missing Patient Reg (Original) A4EL
NOIS	Nursing Service	Inpatient Medications	Order Entry/ Results Reporting
Oncology	Occurrence Screen	Integrated Patient Funds	PCE Patient Care Encounter
PAID	Patch Module	MCCR National Database	Pharmacy Benefits Mangement
Prosthetics	Patient Feedback	Minimal Patient Dataset	Pharmacy Data Management
QUASER	Police & Security	National Laboratory Test	Pharmacy National Database
RPC Broker	Problem List	Network Health Exchange	Pharmacy Prescription Practice
SAGG	Progress Notes	Outpatient Pharmacy	Quality Assurance Integration
Scheduling	Record Tracking	Patient Data Exchange	Quality Improvement Checklist
Social Work	Registration	Patient Representative	Radiology/ Nuclear Medicine
Surgery	Run Time Library	PCE Patient/ HIS Subset	Release of Information - DSSI
Toolkit	Survey Generator	Security Suite Utility Pack	Remote Order/ Entry System
Unwinder	Utilization Review	Shift Change Handoff Tool	Utility Management Rollup
VA Fileman	Visit Tracking	Spinal Cord Dysfunction	CA Vertified Components - DSSI
VBECS	VistALink Security	Text Integration Utilities	Vendor - Document Storage Sys
VDEF	Women's Health	VHS & RA Tracking System	Visual Impairment Service Team ANRV
VistALink		Voluntary Timekeeping	Voluntary Timekeeping National

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: Minor Applications

Which of these are sub-components of your system?

1184 Web
A4P
Administrative Data Repository (ADR)
ADT
Agent Cashier
Air Fortress
Auto Instrument
Automated Access Request
BDN 301
Bed Board Management System
Cardiff Teleform
Cardiology Systems (stand alone servers from the network)
CHECKPOINT
Clinical Data Repository/Health Data Repository
Combat Veteran Outreach
Committee on Waiver and Compromises
CP&E
Crystal Reports Enterprise
Data Innovations
DELIVEREX
DICTATION-Power Scribe
DRM Plus
DSIT
DSS Quadramed
EDS Whiteboard (AVJED)
EKG System
Embedded Fragment Registry
ENDSOFT
Enterprise Terminology Server & VHA Enterprise Terminology Services
ePROMISE
EYECAP
Financial and Accounting System (FAS)
Financial Management System
Genesys
Health Summary Contingency
ICB
KOWA
Lynx Duress Alarm
MHTP
Microsoft Active Directory
Microsoft Exchange E-mail System
Military/Vet Eye Injury Registry
Mumps AudioFAX
NOAHLINK
Omnicell
Onvicord (VLOG)
Optifill
P2000 ROBOT
PACS database
Personal Computer Generated Letters
PICIS OR
PIV Systems
Q-Matic
QMSI Prescription Processing
RAFT
RALS
Remedy Application
SAN
Scanning Exam and Evaluation System
Sentillion
Stellant
Stentor
Tracking Continuing Education
Traumatic Brain Injury
VA Conference Room Registration
VAMedSafe
VBA Data Warehouse
VHAHUNAPP1
VHAHUNFPC1
VISTA RAD
Whiteboard

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: Final Signatures

Facility Name: CDCO > AITC > VHA > National Canteen Service > VCS AIS

Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	512-326-6217	amy.howe1@va.gov
Amy J. Howe — Digital Signature Block	Digitally signed by: Amy J. Howe DN: CN = Amy J. Howe C = US O = U.S. Government OU = Department of Veterans Affairs Date: 2010.12.02 13:37:19 -06'00'		
Information Security Officer:	Thomas P. Johnson	314-845-1446	Thomas.P.Johnson@va.gov
Thomas P. Johnson — Digital Signature Block	Digitally signed by: Thomas P. Johnson DN: CN = Thomas P. Johnson C = US O = U.S. Government OU = Department of Veterans Affairs Date: 2010.12.02 11:18:35 -06'00'		
System Owner/ Chief Information Officer:	John Rucker	512-326-6422	john.rucker@va.gov
Digital Signature Block			
Information Owner:	Craig Caruso	314-845--1340	craig.caruso@va.gov
Digital Signature Block			
AITC Program Manager	Cindy Mack	512-326-6584	cindy.mack@va.gov
Digital Signature Block			

Date of Report:	11/17/10
OMB Unique Project Identifier	029-00-02-00-01-1120-00
Project Name	CDCO > AITC > VHA > National Canteen Service > VCS AIS

(FY 2011) PIA: Final Signatures

Facility Name: AITC

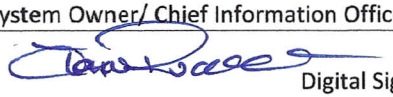
Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	512-326-6217	Amy.Howe1@va.gov

Digital Signature Block

Information Security Officer:

Digital Signature Block

System Owner/ Chief Information Officer:	John Rucker	512-326-6422	John.Rucker@va.gov



Digital Signature Block

Information Owner:

Digital Signature Block

Other Titles:

Digital Signature Block

Date of Report:

OMB Unique Project Identifier

Project Name